

CLAIMS

1. Process for creating and managing pairs of asymmetrical cryptographic keys and associated certificates, each pair of keys being intended for a subject managed by a computer system (1), characterized in that it consists of:

- searching in storage means (7) for at least one subject for which a pair of asymmetric keys and an associated certificate must be created;
- creating at least one individual request for creating and certifying a pair of asymmetric keys for said subject;
- transmitting a request corresponding to said individual creation and certification request to a key generating center (8), which issues a pair of asymmetric keys in accordance with said request;
- creating at least one individual request for certifying the public key created for said subject;
- transmitting a request corresponding to said individual certification request to a certification authority (12), which issues a certificate in accordance with said request.

2. Process according to claim 1, characterized in that a pair of keys must be created for a given subject when said subject lacks a pair of keys and a corresponding individual creation and certification request, or when a pair of keys has been requested for said subject, or when the certificate of a pair of keys for said subject intended for an identical use has been revoked and a new pair of keys has been requested.

3. Process according to either of claims 1 and 2, characterized in that it is executed periodically.

4. Process according to any of claims 1 through 3, characterized in that it creates each individual request from a corresponding multiple creation and certification request stored in the storage means (7) relative to a set of subjects belonging to a preset list or to a set of subjects

defined by predetermined criteria, as well as to model pairs of keys and associated model certificates for the set in question.

5. Process according to claim 4, characterized in that it consists of searching in each of the multiple creation and certification requests of the system for all of the subjects in a condition such that a pair of keys must be created.

6. Process for creating and managing certificates for pairs of asymmetrical cryptographic keys, each certificate being intended for a pair of asymmetrical cryptographic keys for a subject managed by a computer system (1), characterized in that it consists of:

- searching in storage means (7) for at least one pair of asymmetric keys for the public key for which a certificate must be created;
- creating at least one individual request for certifying the public key;
- transmitting a request corresponding to said individual certification request to a certification authority (12), which issues a certificate in accordance with said request.

7. Process according to claim 6, characterized in that a certificate must be created for a given subject when said subject lacks a certificate and an individual certification request, or when a certificate has been requested for said subject, or when the certificate of a pair of keys for said subject expires, or when the certificate of a pair of keys has been revoked.

8. Process according to either of claims 6 and 7, characterized in that it is executed periodically.

9. Process according to claims 7 and 8, characterized in that a certificate must be created for a given subject when the certificate expires during this period.

10. Process according to any of claims 6 through 9, characterized in that it creates each individual request from a corresponding multiple certification request recorded in the

3 storage means (7) relative to a set of pairs of keys for subjects belonging to a preset list or to a set
4 of pairs of keys for subjects defined by predetermined criteria, as well as to associated model
5 certificates for the set in question.

1 11. Process according to claim 10, characterized in that it consists of searching in
2 each of the multiple certification requests of the system for all of the subjects in a condition such
3 that a certificate must be created.

1 12. Process according to any of claims 1 through 6, characterized in that each multiple
2 request comprises an attribute relative to at least one execution date and in that said process
3 consists of including in the search only the multiple requests whose expiration date has arrived.

1 13. Process according to any of claims 1 through 6, characterized in that it consists of
2 performing the encoding of one or more extensions in accordance with one or more given rules
3 and of entering the encoded extension or extensions into the individual certification request
4 during the creation of the latter.

1 14. Process according to any of claims 1 through 6, characterized in that it consists of
2 changing the value of an attribute contained in each of the individual requests in order to indicate
3 its status.

1 15. Computer system (1) that makes it possible to create and manage objects,
2 particularly pairs of asymmetrical cryptographic keys and certificates associated with the pairs of
3 keys, the pairs of keys and the certificates being intended for subjects managed by said system,
4 characterized in that it comprises means for automating the creation and/or certification of at
5 least one pair of keys for each subject managed by the system (1).

1 16. Computer system (1) according to claim 15, characterized in that it comprises at
2 least:

- a central management service (3) capable of creating, updating and consulting the objects and the subjects managed by said system;
 - a local registration authority (5) capable of handling the creation and/or the certification of keys intended for an object;
 - a central security base (7) containing the subjects and objects managed by the system with which the local registration authority communicates;
 - a key generating center (8) capable of creating at least one pair of keys at the request of the local registration authority (5) with which it communicates;
- the system (1) having access to at least one certification authority (12) capable of creating a certificate at the request of the local registration authority (5).

17. Computer system according to either of claims 15 and 16, characterized in that it comprises a mechanism (6) for periodically waking up the local registration authority (5).

18. Process for creating and managing symmetrical cryptographic keys, each key being intended for a subject managed by a computer system (1), characterized in that it consists of:

- searching in storage means (7) for at least one subject for which a symmetric key must be created;
- creating at least one individual request for creating a symmetric key for said subject;
- transmitting a request corresponding to said individual creation request to a key generating center (8), which issues a symmetric key in accordance with said request.

19. Computer system (1) that makes it possible to create and manage objects, particularly symmetrical cryptographic keys, the keys being intended for subjects managed by said system, characterized in that it comprises means for automating the creation of at least one key for each subject managed by the system (1).

add B2